Complying with Data Protection Law in a Changing World

Benjamin Wright
For many enterprises, data protection compliance is a juggling act as they handle data that is subject to laws of many different jurisdictions, with little consistency from place to place. In addition, many enterprises' trading partners impose data compliance rules by way of contracts and industry standards. As diverse stakeholders compete to claim that their rules supersede others, compliance grows increasingly complicated.

In this noisy world of mandates and standards, this paper provides practical advice for decision makers. It identifies major themes of compliance that carry weight around the world. It observes that with strong leadership, a large enterprise can make strides in showing to stakeholders that it is accountable for data and regulating its own use and protection of that data. It can deploy advanced technologies such as cloud security, data loss prevention and insider threat protection to substantiate what is happening to data and to safeguard it from abuse.

This paper also recommends that an enterprise invest in an executive champion who can demonstrate to outsiders that the enterprise is performing responsibly. It stresses how risk assessments can provide better focus to a data compliance plan. At the same time, the paper teaches that an enterprise on the global stage must choose words judiciously when describing its well-intentioned efforts to achieve compliance.

Effective data security can help businesses attract and retain corporate customers. Security is indicative of quality management and service.
Legal and political expectations for data security are rapidly evolving across the world. In general these expectations are calling for greater control over personal information. Examples of this evolution are the European Union’s new General Data Protection Regulation (GDPR),\(^1\) new cyber security regulation issued by the New York Department of Financial Services\(^2\) (applicable to financial institutions) and increasingly common requirements for data security imposed by contracts between business partners.

These changing expectations are emerging at a time when public attention is focused on data security breaches. High-profile breaches and attacks such as those experienced recently by UK healthcare providers, the Central Intelligence Agency and the Democratic Party in the U.S. (including Hillary Clinton’s 2016 presidential campaign) engender anxiety among citizens, politicians and trading partners.

In the context of these events, large enterprises have access to ever-greater quantities of sensitive data. Increasingly this data is processed across networks that cross borders and even span the globe. For many enterprises, the legal and political demands of security can be perplexing. These demands come from many different countries and legal domains, which do not speak with a unified voice. The demands can conflict, or the legal domains can expect different methods to be used to achieve similar outcomes. The demands change over time, so that action deemed to be in compliance this year might not be in compliance next year.

---


The arrival of the new Republican administration in the United States raises some uncertainty about the direction of cyber regulation by the US federal government. Although the Trump administration has signaled that it is serious about cyber security, it also shows a bent toward reduced regulation of private enterprises. The intent for reduced regulation contrasts starkly with the approach of the prior administration. It is unclear how the Trump administration will change regulation and enforcement under such laws as the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley-Act (GLBA) and the Federal Trade Commission Act.

Unfortunately, in this tumult, no sizable enterprise can achieve perfect compliance in every applicable domain. But there are methods to lower the risks of noncompliance. This paper identifies major steps a large multinational enterprise can take to assure the public, business partners and government authorities that it is behaving responsibly and is on a commendable path of compliance.

To contribute to that assurance, advanced technologies are becoming available, as this paper will explain.

---


Many countries require protection of personal information by law. Such laws are expanding quickly, as evidenced by the aggressive new GDPR and related developments in Europe, as well as by recent legislation in Israel and Australia.

At the same time, industry standards (such as the Payment Card Industry Data Security Standard, or PCI-DSS), cyber insurance policies and contracts between enterprises and their trading partners come with their own demands for data protection. It is increasingly common that hospitals, corporations and universities require by contract that their business associates protect sensitive data. These contractual requirements can be highly specific, requiring the protection of both personal data and intellectual property. (See “Cyber Security Questionnaires” at the end of this paper.)

Similarly, government agencies such as tax authorities impose security standards on their business associates that possess or access sensitive information.

Furthermore, corporate boards of directors are holding executives accountable for failing to implement adequate data security. The supervisory board of an Austrian aircraft parts maker recently fired its CEO and CFO after hackers spoofed the CEO’s email and got the company to send out $46 million in unauthorized wire transfers. Similarly, the CEO of a large retailer resigned in the wake of its massive data security breach in 2013.

Spectacular breaches such as those at a large Internet service provider and a large health insurer have motivated more private enterprises to seek cyber insurance. The procurement of cyber insurance in turn imposes a new cyber security discipline on many enterprises. In order to purchase and maintain insurance policies, enterprises must disclose their security practices and then comply with ongoing security standards.

Beyond legal requirements, a data security breach is damaging to an enterprise’s reputation, whether the breach becomes public by way of self-reporting, whistleblowers or third-party analysis. (Brian Krebs, a well-known blogger, sometimes reports a breach discerned by third-party analysts even before the victim has discovered it.) This process of publicly shaming an enterprise data holder for a breach is a powerful force for imposing security expectations.
Nonuniform Expectations

This multitude of diverse expectations for data protection is challenging for larger multinational enterprises. Expectations are far from uniform, and different expectations are subject to interpretation. Disagreements are common about what expectations apply to particular data and which controls take priority over others.

Particular Prescriptive Controls

For example, New York’s new cyber security regulation emphasizes that financial institutions should conduct penetration testing. Meanwhile, Massachusetts’ data protection regulation emphasizes the encryption of data on laptops and other mobile devices. But a multinational enterprise subject to both of these laws—as well as many other legal expectations around the world—may responsibly determine that penetration testing and mobile encryption are not needed as urgently as other controls. The enterprise is forced to exercise judgment and spend its limited time and resources to concentrate on the controls that are most effective, rather than the prescriptive controls mandated by the laws of particular jurisdictions.

Broad, General Requirements with No Guidance

Conversely, some laws around the world state legal expectations in extremely general terms, which provide enterprises little if any guidance on what actually constitutes compliance with those expectations. For example, a Connecticut statute stipulates:

“Any person in possession of personal information of another person shall safeguard the data, computer files and documents containing the information from misuse by third parties.” This is just one of innumerable laws around the world that might apply to the data held by a larger enterprise. It broadly requires the enterprise to “safeguard” data, but it does not explain what safeguard means. It does not explain how far the enterprise must go to safeguard data. It gives no hint as to when compliance has been achieved, in a world where it is impossible to safeguard data perfectly.


What is more, the statute defines the information to be safeguarded in terms that are breathtaking in their scope. Section 1(c) explains that “‘personal information’ means information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a driver’s license number, a state identification card number, an account number.” This definition seems to embrace any kind of imaginable identifier associated with a person. In the digital age, an endless array of data components (including patterns of behavior, lists of friends, styles of writing and much more) could, in the right context, constitute an “identifier” that must be safeguarded. For a large enterprise, this expansive definition is bewildering. The enterprise cannot discern with much certainty what it is expected to safeguard under Connecticut law.

This is just one statute in one U.S. state. A sizable enterprise could face this statute while at the same time confronting hundreds of other obligations for data protection in other jurisdictions around the world.

**Legal Hold Versus Requirement to Destroy**

Yet another legal requirement may expect a different approach to data protection. In the US and other countries, a party is expected to apply a so-called legal hold on records that are subject to litigation and make sure they are not destroyed and are available to be used as evidence in the litigation. So in *IO Group Inc. v. GLBT Ltd.*, a US court punished a website owner in the United Kingdom for intentionally destroying emails and other records relevant to copyright litigation in the US. The website owner argued that the UK Data Protection Act 1998 required destruction of the records because they contained personally identifiable information that was no longer needed for business. The court rejected the argument and held that the website owner had wrongfully destroyed records that should have been retained for pending litigation.

---

Despite the confusion, common global themes for data protection are discernible and can help an enterprise target its data protection program. These themes can help an enterprise make a worldwide case that it is in fact behaving responsibly and striving commendably toward compliance, even though it is not achieving perfection with every expectation, everywhere, all at once.

Eight broad themes are fairly common around the world:

- **Access.** Prevent unauthorized access to personal data, intellectual property and the systems that contain them. Safeguard data from outside intruders and rogue insiders. Avoid suffering a breach.

- **Accountability.** Be accountable for data. Know what you have, why you have it, where it is and what you are doing with it.

- **Proof.** Document your data management and your efforts at compliance. Documentation is objective evidence that can give assurance to auditors, regulators and trading partners.

- **Notification.** Be prepared to give notice if a breach happens. Notice might go to data subjects, business partners and/or government authorities.

- **Action.** Invest professional attention and diligence into the data security problem. Go beyond best practices and the mere installation of technical controls so that you can stay ahead of emerging threats and avoid a debilitating breach or disruption. This can include assigning qualified security staff to actively monitor systems, looking for clues that an intrusion has happened and then disrupting attacks.

- **Self-regulation.** Regulate your own data security practices. Maintain an ongoing, well-resourced process for evaluating your data protection and improving it constantly. Establish that you are not waiting for an authority to investigate you and force you to institute measures to protect data.

- **Insistence.** Insist that your vendors invest in good security too so that they do not infect you or mishandle your data. Audit them.

- **Leadership.** Appoint responsible leadership for compliance. Designate a qualified officer to lead your privacy and data protection team, and give that officer the necessary budget and authority.
These themes are not a comprehensive checklist for every enterprise. Many enterprises will be wise to place greater emphasis on particular compliance steps due to their exposure in a particular jurisdiction or industry sector. But these eight broad themes are instructive for enterprises that struggle under multiple compliance mandates across several countries and numerous industries.

**Technology Campaigns for Compliance**

We have identified three major technology campaigns available to larger enterprises that are growing in maturity. These technology campaigns can help an enterprise make the case that it maintains a commendable process for compliance with the aforementioned major themes. By making that case, an enterprise establishes that it is a good steward of sensitive data. The three technology campaigns are cloud security, data loss prevention and protection from insider threats.

- **Cloud Security**

Cloud technology causes data to scatter and move. In simple terms, effective cloud security can do the following:

- Tell you what data you have, where it is located and what is happening with it.
- Facilitate accountability for data.
- Discover and map the data across the cloud or across network boundaries.
- Keep audit trails about the data’s acquisition and status.
- Monitor and record access to data and workloads that process the data.
- Monitor how the data is being handled, as well as how and when the data might be destroyed.
- Confirm that data has been retained when required by law or policy.

Knowledge of the geographic location of data can be relevant to determining what laws apply to the data. It can be critical when laws or standards demand that data stay within a specified jurisdiction (country or group of countries).

Effective cloud security can help prevent unauthorized access to data and keep records of compliance with policies and legal obligations. If unauthorized access does occur, cloud security can provide logs and audit trails for assessing the incident and determining whose data was accessed so that those directly affected can be notified, as required by law.
**Data Loss Prevention**

Broadly speaking, data loss prevention (DLP) looks for evidence that data might be departing its authorized locations or workloads and initiates steps to prevent or limit that departure. Competent DLP accomplishes the following:

- Identifies protected data by characteristics or fingerprints.
- Monitors network traffic for clues showing the data is in the wrong place, is being exfiltrated or is being processed under unauthorized workloads. The clues might include abnormal user or machine behavior.
- Logs access to data and maintains records of its work so that its performance can be audited and confirmed to outsiders. These logs and records can facilitate responses to security incidents or investigations into suspected data breaches.
- Helps the data holder prove to an auditor or the data owner (such as a corporate customer that insists on security by way of contract) that data security has not been compromised.
- Can stop an attack before it starts or limit its impact if it does start.

**Protection from Insider Threats**

Technology for safeguarding data from insiders recognizes that the endpoints controlled by enterprise staff are often weak points. Some insiders become bad actors, while others are simply careless—or unlucky—and allow their devices to be compromised.

A mature insider threat campaign does the following:

- Seeks to monitor endpoints such as PCs or mobile devices for suspicious behavior or unauthorized functionality.
- Can enable an enterprise to compare past behavior of an endpoint with current behavior and automatically signal to the security team when special attention is needed.
- Can help head off a data security breach or contain it before it enlarges.

The presence of insider threat protection can deter rogue insiders because they know their misdeeds can be detected, stymied and reported. Insider threat protection is emblematic of self-regulation that can reassure stakeholders such as regulators or trading partners.
For most large enterprises, compliance is a constant work in progress. At any given time, the enterprise is working on many projects that handle sensitive data in different jurisdictions around the world. Many such projects have legacies that stretch back for years or decades. So it is hard for the enterprise to follow a textbook plan for achieving compliance. It will make progress in some areas faster than in other areas.

Still, a general plan for compliance provides direction for the entire enterprise.

**Designate an Internal Champion**

The most critical step in implementing a complex compliance plan is to designate a champion. A champion is an internal leader who will win approval for the plan from executive management. He or she should be a credible individual who profoundly understands what is at stake and who will devote the time and energy necessary to push a plan forward. A champion might be an existing member of executive management, a senior manager from the legal or compliance staff or a specially hired data protection officer.

Regardless of his or her background, the champion must explain to officers and directors the urgency of the problem caused by noncompliance. The champion can point to sensational stories such as recent breaches and attacks at large government agencies and major media companies. The conversation can cover how noncompliance under the GDPR, for example, could potentially lead to fines of unthinkable proportions. Marshaling convincing facts illustrates that all enterprises risk their most valuable assets—their brand and their reputation—if they fail to secure data and manage it responsibly.

An effective champion does more than win senior management’s support, budget and resources for a compliance plan. He or she sustains that relationship with senior management, reminding them how critical it is to implement the compliance plan and constantly improve on it.
Assess Risk and Act Accordingly

A champion ensures that a team is assembled and priorities are set. No enterprise will get close to doing compliance all at once. But risk assessments can help to identify what steps, policies and technologies demand the most immediate attention. Many of the legal expectations for data protection recognize the importance of a risk assessment and action that is based on the areas of highest risk. For example, Article 32 of the GDPR emphasizes that the degree of effort invested in a particular security measure must be informed by the risk present in a particular setting or application.17

Similarly, in the United States, the Department of Health & Human Services (HHS) emphasizes the role of risk analysis in guiding compliance with data security requirements under HIPAA.18 HHS recently fined a network of healthcare providers $400,000 for failing to conduct an adequate risk analysis and then implement a risk management plan to protect health information.19

An effective champion will follow up to confirm that qualified teams are deployed to analyze risk and then use that analysis to develop and implement appropriate policies or procedures across the enterprise. The development and implementation of policies and procedures is a task that varies from one enterprise to the next and from one division within an enterprise to another. Fill-in-the-blank, cookie-cutter form policies are often ineffective. Policy development requires professional attention, as do the periodic review and updating of policies and procedures. Policies and procedures must be tailored to fit particular risks, technologies and local legal expectations.


Write Accurate Policies and Procedures

As enterprises write policies and procedures, they are wise to avoid overpromising by steering away from absolute statements such as, “We will implement …” firewalls, data loss prevention or other technologies that meet certain standards. Always implementing particular technologies or procedures is very hard to do in practice. The threat landscape is changing too quickly, and the services and functionality demanded by users and customers are changing too quickly.

Therefore, an enterprise is prudent to write more accurate language into its policies, such as saying that the enterprise “strives to implement” particular technologies or procedures.20 In this regard, the “privacy vision” of a global database provider is instructive. Observe the words the company publishes on its website (emphasis added):

“[The company] strives to protect personally identifiable information that we maintain or disseminate, including through the use of appropriate administrative, physical, and technical safeguards.

“We aspire to protect individuals’ privacy through the design of our products, by credentialing, monitoring, and auditing our customers as appropriate, and through other information security safeguards.”21

Words such as strive and aspire candidly acknowledge the challenges of data protection, while displaying earnest intention to work expeditiously on the problems. The words imply an unending process of improvement, but never the attainment of perfection.

Align Policy, Process and Technology

Given that data compliance and security are always works in progress, it is hard to keep policies, processes and technologies in alignment. But constant vigilance over that alignment reduces risk: the risk that the enterprise will default on its legal obligations, and the risk that the enterprise will fall victim to an attack.

The writing of policies sets goals, but to reach those goals, you must have effective processes, backed up with effective technology. In the current tumultuous environment, goals should be stated in relatively general, nonprescriptive terms so that the processes and technologies can evolve quickly to address the risks.

---


Successful compliance entails more than the implementation of technologies or rote adherence to a checklist of security measures. It requires professional attention and judgment, as well as compromise and tradeoffs. It demands a rigorous, continuous process of testing and upgrading.

But in a fluid compliance landscape, the deployment of mature tools by a professional, well-led team can be impactful. It can help to convince outside observers that the enterprise is ahead of its peers and deserving of less scrutiny, as well as a passing grade on many measures of compliance.

Maintenance of a strong security posture achieves more than compliance with legal requirements. It reduces the risk of a debilitating data breach or cyber attack. More importantly, a strong security posture fosters confidence on the part of trading partners such as corporate customers. For customers, the security of a vendor is a symbol of quality. When a customer perceives that a vendor is secure, the customer has reason to believe the vendor is well-managed and likely to support a successful relationship.
Cyber security questionnaires are an increasingly common method for imposing legal expectations for security. For example, many large organizations such as corporations and government agencies expect their vendors to answer detailed questionnaires about how the vendors protect data. Cyber insurers request similar questionnaires from prospective purchasers of commercial insurance policies.

These questionnaires and the answers submitted imply legal obligations. If a vendor mischaracterizes its security posture to a prospective corporate customer, for example, that customer might later claim that the vendor committed legal fraud or misrepresentation. In other words, the customer would say, “You lied to me.” The respondents to these questionnaires must therefore be very careful to answer accurately, without representing their security program as being more than it truly is. Respondents are wise to assign senior staff to answering these questionnaires to ensure accuracy.

It is critical to understand, however, that these questionnaires do more than impose legal obligations. Today they enable an organization to assess a prospective vendor in a new way. They give the customer visibility into the vendor’s response to a challenging issue: information security. Good security implies that the vendor is competently managed and therefore likely to deliver good service across the entire relationship with the customer.

Following are sample questions drawn from questionnaires circulated by large institutions to vendors or prospective vendors. Notice how broadly written these questions are. They seem to be requesting a tremendous amount of specific technical and management information. Observe, too, that submitting short, simplistic answers can be a mistake, because such answers tend to be overly sweeping. It would be easy, for instance, for a respondent to suggest that something (such as data tracking) always happens when in truth it almost always happens—but not absolutely always.

- Describe the security features incorporated into information resources to be provided or used by prospective vendor pursuant to this request for proposal.
- Describe the monitoring procedures and tools used for monitoring the integrity and availability of all products interacting with information resources, including procedures and tools used to detect security incidents and to ensure timely remediation.
• Does prospective vendor have a data backup and recovery plan, supported by policies and procedures, in place for information resources? If yes, briefly describe the plan, including scope and frequency of backups, and how often the plan is updated. If no, describe what alternative methodology the prospective vendor uses to ensure the restoration and availability of customer records.

• Are reasonable physical security and environmental controls present in the building/data center that contains relevant systems and data? If so, do those controls include:
  - Access restricted and logs kept of all access? If yes, please describe how.
  - Perimeter physical barrier (such as fence or walls)? If yes, please list all types.
  - Physical access control procedures? If yes, is there:
    • Segregation of duties for issuing and approving access to the facility (keys, badge, etc.)?
    • Access reviews at least every six months? If yes, please provide evidence.

• Do external parties have access to relevant systems and data or processing facilities? If so, is:
  - Access prohibited prior to a risk assessment being conducted?
  - A risk assessment performed on third parties?
Following are two real-world case examples that demonstrate how to improve compliance. Each example describes an enterprise struggling to address complex data protection requirements. In each case, the enterprise implements technology under strict specifications to promote compliance.

**IT Services Provider Upgrades Data Loss Prevention**

An IT services provider supported enterprise customers in North America, Europe and Asia Pacific. Customers from retail, banking, insurance, healthcare and manufacturing relied on the provider to process and protect their data.

The provider needed uniformity in its data security practices across the globe so that it could satisfy audits by and expectations of its global customers. But satisfying those audits and expectations was a challenge as its employees traveled from one facility to another and used a growing array of devices to access the provider’s network.

The provider had suffered an incident involving data leakage when an employee logged into the network from a remote computer and sent to a customer emails containing sensitive data; the data should have been handled by a more secure method than standard email. This incident showed that the provider’s systems administrator needed more complete and consistent visibility of what was happening. The provider needed to be able to monitor where user data was going in order to prevent data loss and data theft.

In response, the provider deployed an advanced data loss prevention solution in its global network. The solution allowed an administrator to manage all policies and reporting from a single console. Additionally, the solution consolidated management of cloud-based and on-premises security.

The result: The provider’s director of IT is now better able to assure customers that all of their data, including data in remote offices, is secure.
Cloud Security Solution Needed to Safeguard Personal Data

A firm provided psychological well-being services to the employees of its corporate clients. The clients, who came from various industry sectors in the United Kingdom, expected the firm’s network to be secure, because it possessed sensitive personal information pertaining to client employees.

Yet the firm had fallen victim to two advanced crypto-ransomware attacks. It knew it needed to improve security.

The firm sought a best-in-class cloud security solution with superior functionality and performance. Through systematic due-diligence research and pilot testing, the firm found a cloud security solution that enabled it to identify and regulate advanced threats such as crypto-ransomware.

The solution included scalable sandbox technology for cloud-based web and email security. The firm can monitor web traffic for real-time code analysis in a behavioral sandbox for advanced threat identification. In addition, email sandboxing allows for interception of attachments in real time for additional threat analysis in order to identify targeted attacks. The two ransomware attacks that had hit it had been executed via email attachments.

The result: The firm can give greater assurances to its clients that sensitive data will be safeguarded.
Benjamin Wright is a practicing attorney based in Dallas, Texas, focusing on technology law. He serves as a senior instructor at the SANS Institute, teaching its five-day course, “Law of Data Security and Investigations.” By means of that course, Mr. Wright has taught thousands of students from throughout the world. He chairs the SANS Institute’s annual Data Breach Summit. Benjamin advises diverse clients, both in the United States and outside of it, on privacy, electronic commerce and data security law. http://benjaminwright.us

This paper provides general, summary education to the public. It does not provide legal advice for any particular situation. The reader should not rely on this paper as a complete or accurate statement of law. If the reader needs a complete and accurate statement of law, or legal advice for a particular situation, then the reader should consult a competent lawyer.
# Upcoming SANS Training

Click here to view a list of all SANS Courses

<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>Dates</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Miami 2020</td>
<td>Miami, FLUS</td>
<td>Jan 13, 2020 - Jan 18, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cyber Threat Intelligence Summit &amp; Training 2020</td>
<td>Arlington, VAUS</td>
<td>Jan 20, 2020 - Jan 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam January 2020</td>
<td>Amsterdam, NL</td>
<td>Jan 20, 2020 - Jan 25, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Anaheim 2020</td>
<td>Anaheim, CAUS</td>
<td>Jan 20, 2020 - Jan 25, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>MGTS21 Beta Two 2020</td>
<td>San Diego, CAUS</td>
<td>Jan 22, 2020 - Jan 23, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Francisco East Bay 2020</td>
<td>Emeryville, CAUS</td>
<td>Jan 27, 2020 - Feb 01, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas 2020</td>
<td>Las Vegas, NVUS</td>
<td>Jan 27, 2020 - Feb 01, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Vienna January 2020</td>
<td>Vienna, AT</td>
<td>Jan 27, 2020 - Feb 01, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security East 2020</td>
<td>New Orleans, LAUS</td>
<td>Feb 01, 2020 - Feb 08, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS New York City Winter 2020</td>
<td>New York City, NYUS</td>
<td>Feb 10, 2020 - Feb 15, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA - Fairfax 2020</td>
<td>Fairfax, VAUS</td>
<td>Feb 10, 2020 - Feb 15, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dubai February 2020</td>
<td>Dubai, AE</td>
<td>Feb 15, 2020 - Feb 20, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Scottsdale 2020</td>
<td>Scottsdale, AZUS</td>
<td>Feb 17, 2020 - Feb 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Diego 2020</td>
<td>San Diego, CAUS</td>
<td>Feb 17, 2020 - Feb 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Brussels February 2020</td>
<td>Brussels, BE</td>
<td>Feb 17, 2020 - Feb 22, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Open-Source Intelligence Summit &amp; Training 2020</td>
<td>Alexandria, VAUS</td>
<td>Feb 18, 2020 - Feb 24, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Training at RSA Conference 2020</td>
<td>San Francisco, CAUS</td>
<td>Feb 23, 2020 - Feb 24, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Jacksonville 2020</td>
<td>Jacksonville, FLUS</td>
<td>Feb 24, 2020 - Feb 29, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Manchester February 2020</td>
<td>Manchester, GB</td>
<td>Feb 24, 2020 - Feb 29, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Zurich February 2020</td>
<td>Zurich, CH</td>
<td>Feb 24, 2020 - Feb 29, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2020</td>
<td>Bangalore, IN</td>
<td>Feb 24, 2020 - Feb 29, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>Blue Team Summit &amp; Training 2020</td>
<td>Louisville, KYUS</td>
<td>Mar 02, 2020 - Mar 09, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA - Reston Spring 2020</td>
<td>Reston, VAUS</td>
<td>Mar 02, 2020 - Mar 07, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Japan 2020</td>
<td>Tokyo, JP</td>
<td>Mar 02, 2020 - Mar 14, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich March 2020</td>
<td>Munich, DE</td>
<td>Mar 02, 2020 - Mar 07, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS St. Louis 2020</td>
<td>St. Louis, MOUS</td>
<td>Mar 08, 2020 - Mar 13, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Austin Winter 2020</td>
<td>OnlineTXUS</td>
<td>Jan 06, 2020 - Jan 11, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>

Last Updated: December 23rd, 2019